

FORTUNE**Why Cryptojacking Is The Next Big Cybersecurity Threat**

By **ROBERT HACKETT** Updated: January 9, 2018 1:38 PM ET | Originally published: October 23, 2017

Meet the Internet's latest menace. Hackers and penny-pinching website hosts are hijacking people's computers to "mine" cryptocurrency. And we're not talking about coal and canaries.

Cryptocurrency is mined, or produced, by solving complex mathematical puzzles. It's like a lottery: The more computing power you throw at the problems, the likelier you are to win a reward. Every so often, a computer finds a solution and strikes (digital) gold.

The moneymaking phenomenon is more common than you might think. CBS's Showtime [reportedly ran cryptominer tech](#) on viewers' PCs this year, removing it after security researchers called it out in September. (A Showtime spokesperson declined to comment to *Fortune*.) The mining code later appeared temporarily on the official website of soccer star Cristiano Ronaldo. (A spokesperson could not be reached.) The Pirate Bay website, host of many links to copyright-infringing files, also tested a cryptominer without telling its audience. After an outcry, the site's operators [said in a public note](#) that they were experimenting with alternatives to ads as a source of revenue. Industry watchers have speculated that hackers may have been at work in some instances, planting the crypto code on popular sites and forcing people's machines to generate virtual currency for them.

[Bitcoin](#), the original cryptocurrency, now requires customized chips, bespoke hardware, and large, centralized server farms to mine—far beyond what a gaggle of PCs can offer. But as newer, gaming-resistant cryptocurrencies have sprouted the "cryptojacking" trend has started to make a comeback.

The resurgence can be attributed to the cryptocurrency Monero, which arrived on the scene in 2014. Designed to be mined on PCs, the privacy-minded e-coin sparked the development of a handful of off-the-shelf Monero mining tools, such as Coinhive and Crypto-Loot. When added to a website, these tools transform typically unsuspecting visitors' computers into cryptographic quarries—and new revenue streams.

“Ads don’t work that well anymore—plus they are annoying,” says a spokesperson for Coinhive. The project debuted in September, and Coinhive says it has generated a total of 3,200 Monero tokens—worth approximately \$288,000—as of the first week of October. The project takes a 30% cut of the loot, leaving the rest to the tool’s installer.

Maya Horowitz, threat intelligence manager at Check Point, an Israeli cybersecurity giant, [previewed a report](#) on the burgeoning threat exclusively with *Fortune*. Her team found thousands of examples of video-streaming and file-sharing websites hosting cryptomining software like Coinhive. Almost all failed to disclose the tools’ use, she says. “I don’t think any one of these is very safe or good for users,” Horowitz warns, noting that the code can make computers crash and can provide an avenue for hackers to insert their own malicious code.

Karl Sigler, threat intelligence manager at the cybersecurity company Trustwave, agrees. “Having systems freeze, losing data users were working on can have a significant effect on productivity,” he says, mentioning possible side effects of crypto-sapped PC power.

[Get Data Sheet](#), *Fortune’s technology newsletter*.

Coinhive recently created a version of its tool that includes an opt-in button, so people can grant the miner their consent. Even with their permission, it’s hard to imagine the scraggly crew ever toppling the digital ads market, an \$83 billion industry in the U.S. alone, according to researcher eMarketer. In the meantime, if you’re worried about miners manipulating your computer to mint Monero, consider downloading a “blocker” browser extension, like minerBlock or No Coin, or an antivirus program, like Malwarebytes, that has blacklisted the code.

A version of this article appears in the Nov. 1, 2017 issue of Fortune with the headline “To Catch a Cryptothief.”

CORRECTION: *A previous version of this article mistakenly referred to JSEcoin as a Monero miner. It is not. Rather, it mines its own coin—the eponymous JSEcoin.*